UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte CHEUK W. KO

Appeal No. 2005-1667
Application No. 09/593,280

ON BRIEF

Before CRAWFORD, GROSS, and RUGGIERO, Administrative Patent Judges.

CRAWFORD, Administrative Patent Judge.

DECISION ON APPEAL

This is a decision on appeal from the examiner's final rejection of claims 1 to 27, which are all of the claims pending in this application.

We reverse.

The appellant's invention relates to a computer security and intrusion detection system and more specifically to a method for providing content-based intrusion detection for a computer system by using an agile kernel-based auditing system (specification, pages 1 to 2). A copy of the claims under appeal is set forth in the appendix to the appellant's brief.

The Prior Art

The prior art references of record relied upon by the examiner in rejecting the appealed claims are:

Borchardt et al. (Borchardt)	5,513,317	Apr. 30, 1996
Smaha et al. (Smaha)	5,557,742	Sep. 17, 1996
Vu	5,623,601	Apr. 22, 1997
Epstein et al. (Epstein)	6,584,508	Jun. 24, 2003 (filed Dec. 30, 1999)

The Rejections

Claims 1 to 3, 7 to 12, 16 to 21 and 25 to 27 stand rejected under 35 U.S.C. § 103 as being unpatentable over Smaha in view of Borchardt.

Claims 4, 6, 13, 15, 22 and 24 stand rejected under 35 U.S.C. § 103 as being unpatentable over Smaha and Borchardt as applied to claim 1 and further in view of Epstein and Kernighan.

Claims 5, 14 and 23 stand rejected under 35 U.S.C. § 103 as being unpatentable over Smaha and Borchardt as applied to claim 1 and further in view of Vu.

Rather than reiterate the conflicting viewpoints advanced by the examiner and the appellant regarding the above-noted rejections, we make reference to the answer for the examiner's complete reasoning in support of the rejections, and to the brief and reply brief for the appellant's arguments thereagainst.

OPINION

In reaching our decision in this appeal, we have given careful consideration to the appellant's specification and claims, to the applied prior art references, and to the respective positions articulated by the appellant and the examiner. As a consequence of our review, we make the determinations which follow.

We turn first to the examiner's rejection of claims 1 to 3, 7 to 12, 16 to 21 and 25 to 27 under 35 U.S.C. § 103 as being unpatentable over Smaha in view of Borchardt. We initially note that in rejecting claims under 35 U.S.C. § 103, the examiner bears the initial burden of presenting a prima facie case of obviousness. See In re Rijckaert, 9 F.3d 1531, 1532, 28 USPQ2d 1955, 1956 (Fed. Cir. 1993). A prima facie case of obviousness is established by presenting evidence that the reference teachings would appear to be sufficient for one of ordinary skill in the relevant art having the references before him to make the proposed combination or other modification. See In re Lintner,

9 F.2d 1013, 1016, 173 USPQ 560, 562 (CCPA 1972). Furthermore, the conclusion that the claimed subject matter is prima facie obvious must be supported by evidence, as shown by some objective teaching in the prior art or by knowledge generally available to one of ordinary skill in the art that would have led that individual to combine the relevant teachings of the references to arrive at the claimed invention. See In re Fine, 837 F.2d 1071, 1074, 5 USPQ2d 1596, 1598 (Fed. Cir. 1988). Rejections based on § 103 must rest on a factual basis with these facts being interpreted without hindsight reconstruction of the invention from the prior art. The examiner may not, because of doubt that the invention is patentable, resort to speculation, unfounded assumption or hindsight reconstruction to supply deficiencies in the factual basis for the rejection. See In re Warner, 379 F.2d 1011, 1017, 154 USPQ 173, 177 (CCPA 1967), cert. denied, 389 U.S. 1057 (1968). Our reviewing court has repeatedly cautioned against employing hindsight by using the appellant's disclosure as a blueprint to reconstruct the claimed invention from the isolated teachings of the prior art. See, e.g., Grain Processing Corp. v. American Maize-Products Co., 840 F.2d 902, 907, 5 USPQ2d 1788, 1792 (Fed. Cir. 1988).

The appellant's invention, as recited in claim 1, is a method of detecting intrusion into a computer system. The first step is receiving of an audit specification which specifies a target attribute and an auditing criterion (specification at page 7). A target attribute can include any information related to a system call including, for

example, a parameter related to a process making a system call (such as a process of a user ID), data read during a system call and data written during a system call (specification at page 9). A auditing criterion can include any specifier for a condition associated with a system call including a user identifier for a process that is making the system call, an identifier for an application program from which the system call is being made or an identifier for a file being accessed by the system call (specification at page 9). For example, if the target attribute is the data written during a system call and the auditing criterion is a password file, the audit specification would be that the data is being written to a password file.

Once the audit specification is received the method of appellant's invention records the target attribute and produces an audit log (specification at page 10). The audit log is then examined to detect patterns of intrusion (specification at page 10). The size of the audit log may be reduced prior to the examination of the log for patterns of intrusion (specification at page 10.)

The examiner is of the opinion that Smaha describes the invention as recited in claim 1, except that Smaha does not describe that the size of the audit log is reduced prior to the examination of the detection of the patterns. The examiner relies on Borchardt for teaching a trace filter in which data is deliberately filtered according to one or more attributes before being analyzed by a programmer. The examiner concludes:

> . . . it would have be obvious to one of ordinary skill in the art at the time the invention was made to implement the system disclosed by Smaha by deliberately filtering according to one or more attributes before being analysis, as disclosed by Borchardt, as the volume of information provided by a trace facility can grow to such large proportions as to obscure the few relevant pieces of information that the trace facility has captured. [answer at page 6]

Appellant argues that Smaha does not describe the step of receiving an audit specification as required by claim 1.

We find that Smaha describes a method for detecting intrusion or misuse into a computer in which the detection of false positive misuse reports is minimized (col 1, lines 9 to 16). The method of Smaha minimizes the creation of false positive misuse reports by defining a misuse by the use of a signature and signature data structure. A signature is a set of events (security states of the system) and transition functions that define a sequence of actions that form a misuse (col. 5, lines 7 to 12). A signature data structure contains the elements of the signature including an index, an initial state, transition functions, states and an end state that embodies the computer representation of a misuse (col. 8, lines 30 to 35). In operation, Smaha determines whether a misuse has occurred by sending data to a misuse engine which analyzes the data according to the signature data structure. If there is a match, it is determined that a misuse has occurred and the misuse engine sends a signal to an output report mechanism which may send a misuse report to various destinations (col 4, lines 49 to 60).

We agree with the appellant that Smaha does not describe an audit specification. The audit specification of appellant's invention limits the data that is subject to examination to detect intrusion or misuse. Only when the data is a target attribute that fits an auditing criterion is it stored on an audit log and examined for patterns of intrusion or misuse. Smaha does not limit the data that is subject to misuse detection but rather defines what a misuse is by use of a signature data structure so as to limit the presence of false misuses in a misuse report. In addition, Smaha does not form an audit report but rather a misuse report.

We note that even if the examiner is correct that Smaha's generation of a misuse report could be considered the receipt of an audit specification and configuration of an audit log, the log formed by the Smaha method would include misuses or intrusions and there would not be need to perform the next step of "examining the audit log to detect patterns for intrusion" a required by claim 1.

In view of the foregoing, we will not sustain the rejection of claim 1 and claims 2 to 3, 7 to 9 dependent thereon. We will also not sustain this rejection as it is directed to claim 10 and claims 11 to 12, 16 to 18 dependent thereon because claim 10 also requires the receipt of an audit specification and the examination of an audit log for patterns of intrusion. We will likewise not sustain this rejection as it is directed to claim 19 and claims 20, 21 and claims 25 to 27 dependent thereon because claim19 also

requires receiving an audit specification and examination of the audit log to detect intrusions.

We turn next to the examiner's rejection of claims 4, 6 , 13, 15, and 22 to 24 over Smaha in view of Borchardt, Epstein and Kernighan. Recognizing that Smaha does not describe the calls that are included in a target attribute as required by claim 4, the examiner relies on Epstein and Kernighan.

We will not sustain this rejection for the same reasons detailed above for claim 1 because this rejection relies on the teaching of Smaha for teaching the subject matter of independent claims 1, 10 and 19 from which claims 4, 6, 13, 15, and 22 to 24 depend. We have examined the disclosures of Epstein and Kernighan and they do not cure the deficiencies noted above for Smaha.

We turn lastly to the examiner's rejection of claims 5, 14 and 23 under 35 U.S.C. § 103 as being unpatentable over Smaha, Borchardt and further in view of Vu.

We will not sustain this rejection for the same reasons detailed above for claim 1 because this rejection relies on the teaching of Smaha for teaching the subject matter of independent claims 1, 10 and 19 from which claims 5, 14 and 23 depend. We have examined the disclosure of Vu and determined that the disclosure does not cure the deficiencies noted above for Smaha.

The decision of the examiner is reversed.

REVERSED

MURRIEL E. CRAWFORD
Administrative Patent Judge

ANITA PELLMAN GROSS
Administrative Patent Judge

JOSEPH F. RUGGIERO
Administrative Patent Judge

) BOARD OF PATENT
) APPEALS
) AND
) INTERFERENCES

ZILKA-KOTAB, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

MEC